Hindawi
Security and Communication Networks
Volume 2017, Article ID 9289410, 6 pages
https://doi.org/10.1155/2017/9289410

Research Article

Building Secure Public Key Encryption Scheme from Hidden Field Equations

Yuan Ping,[1,2] Baocang Wang,[1,3] Yuehua Yang,[1] and Shengli Tian[1]

[1]*School of Information Engineering, Xuchang University, Xuchang 461000, China*
[2]*Guizhou Provincial Key Laboratory of Public Big Data, Guiyang 550025, China*
[3]*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Baocang Wang; bcwang79@aliyun.com

Received 4 April 2017; Accepted 5 June 2017; Published 10 July 2017

Academic Editor: Dengpan Ye

Multivariate public key cryptography is a set of cryptographic schemes built from the NP-hardness of solving quadratic equations over finite fields, amongst which the hidden field equations (HFE) family of schemes remain the most famous. However, the original HFE scheme was insecure, and the follow-up modifications were shown to be still vulnerable to attacks. In this paper, we propose a new variant of the HFE scheme by considering the special equation $x^2 = x$ defined over the finite field $\mathbb{F}_3$ when $x = 0, 1$. We observe that the equation can be used to further destroy the special structure of the underlying central map of the HFE scheme. It is shown that the proposed public key encryption scheme is secure against known attacks including the MinRank attack, the algebraic attacks, and the linearization equations attacks. The proposal gains some advantages over the original HFE scheme with respect to the encryption speed and public key size.

1. Introduction

Public key cryptography [1] built from the NP-hardness of solving multivariate quadratic equations over finite filed [2, 3] was conceived as a plausible candidate to traditional factorization and discrete logarithm based public key cryptosystems due to its high performance and the resistance to quantum attacks [4]. The hidden field equations (HFE) scheme [5] may be the most famous cryptosystem amongst all multivariate public key cryptographic schemes. The HFE scheme firstly defines a univariate map over an extension field $\mathbb{F}_{q^n}$:

$$\mathcal{F}(X) = \sum_{0\le i\le j<n, q^i+q^j\le D} a_{ij} X^{q^i+q^j} + \sum_{0\le i<n, q^i\le D} b_i X^{q^i} + c, \quad (1)$$

where the degree bound D chosen cannot be very large in order that the user can use the Berlekamp algorithm [6] to efficiently compute the roots of $\mathcal{F}(X)$. Then two invertible affine transformations are applied to hide the special structure of the central map [2, 5]. However, the central map $\mathcal{F}(X)$ can be represented with a low-rank matrix [7], which makes it vulnerable to MinRank attacks [7–9]. So some modifications are needed to repair the basic HFE scheme [10–14]. However, all known modification methods only can impose partial nonlinear transformation on the special structure of the HFE central map, and hence they are still vulnerable to some attacks [15–17].

We consider the HFE scheme over finite fields with characteristic 3. We impose some restrictions on the plaintext space and can use the restriction to merge the coefficients of the linear part and the square part. By doing this, we can impose a fully nonlinear transformation on the central map of the HFE encryption scheme. Performance analysis shows that the modification can save the public key storage by $\mathcal{O}(n^2)$ bits and reduces the encryption costs by about $\mathcal{O}(n^2)$ bit operations. It is shown that the modification can defend the known attacks including the MinRank attack, the linearization equations attack, and the direct algebraic attacks.

2. Proposal

2.1. Notations. Let $\mathbb{F}_q$ be a q-order finite field with q being a prime power. Let $f(x)$ be an irreducible polynomial with degree n over $\mathbb{F}_q$; then $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/\langle f(x)\rangle$ forms a degree-n extension field. The construction admits a standard isomorphism ϕ between the extension field $\mathbb{F}_{q^n}$ and the vector space $\mathbb{F}_q^n$; namely, for an element $g(x) = \sum_{i=0}^{n-1} g_i x^i \in \mathbb{F}_{q^n}$, we have $\phi(g(x)) = (g_0, \ldots, g_{n-1}) \in \mathbb{F}_q^n$. We denote the inverse of map ϕ as ϕ^{-1}. Note that the Frobenius maps $\mathcal{T}(X) = X^{q^i}$ for $i = 0, 1, \ldots, n-1$ defined over $\mathbb{F}_{q^n}$ are $\mathbb{F}_q$-linear; namely, when expressed in the base field $\mathbb{F}_q$, $\mathcal{T}(X)$ will be n-dimensional linear functions over $\mathbb{F}_q$.

2.2. Description. The encryption scheme consists of three subalgorithms: key generation, encryption, and decryption.

Key Generation. The system parameters consist of an irreducible polynomial $f(x)$ with degree n over $\mathbb{F}_3$, the extension field $\mathbb{F}_{3^n} = \mathbb{F}_3[x]/\langle f(x)\rangle$, and the isomorphism ϕ between $\mathbb{F}_{3^n}$ and $\mathbb{F}_3^n$. Firstly, we define an HFE map $\mathcal{F}(X)$ in (1) and randomly choose two invertible affine transformations $\mathcal{L}_1 : \mathbb{F}_3^n \to \mathbb{F}_3^n$ and $\mathcal{L}_2 : \mathbb{F}_3^n \to \mathbb{F}_3^n$. Then we compute their inverses $\mathcal{L}_1^{-1}$ and $\mathcal{L}_2^{-1}$ and the n-variable quadratic polynomials $\mathcal{P} = \mathcal{L}_1 \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ \mathcal{L}_2 = (p_0, p_1, \ldots, p_{n-1})$. For $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, we set

$$p_k(\mathbf{x}) = \sum_{i=0}^{n-1} \alpha_i^{(k)} x_i^2 + \sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} \beta_{ij}^{(k)} x_i x_j + \sum_{i=0}^{n-1} \gamma_i^{(k)} x_i + \delta^{(k)}, \quad (2)$$

where all the coefficients are in $\mathbb{F}_3$ for $k = 0, \ldots, n-1$. Then we merge the coefficients of the square and linear terms of p_k, that is, $\rho_i^{(k)} = \alpha_i^{(k)} + \gamma_i^{(k)}$ for $i, k = 0, 1, \ldots, n-1$, and get the public key of the modified HFE scheme, namely, n quadratic polynomials $\mathcal{Q} = (q_0, q_1, \ldots, q_{n-1})$, where, for $k = 0, \ldots, n-1$,

$$q_k(\mathbf{x}) = \sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} \beta_{ij}^{(k)} x_i x_j + \sum_{i=0}^{n-1} \rho_i^{(k)} x_i + \delta^{(k)}. \quad (3)$$

The secret key consists of $\mathcal{F}(X)$, $\mathcal{L}_1^{-1}$, and $\mathcal{L}_2^{-1}$.

Encryption. The plaintext space is $\mathcal{M} = \{0, 1\}^n$. For a plaintext $\mathbf{m} \in \mathcal{M}$, we just compute $\mathbf{c} = (c_0, \ldots, c_{n-1}) = \mathcal{Q}(\mathbf{m}) \in \mathbb{F}_3^n$ as the ciphertext.

Decryption. Given a ciphertext $\mathbf{c} \in \mathbb{F}_3^n$, we compute $\mathbf{y} = \mathcal{L}_1^{-1}(\mathbf{c})$ and $Y = \phi^{-1}(\mathbf{y}) \in \mathbb{F}_{3^n}$, and we use the Berlekamp algorithm [6] to compute all the preimages $X \in \mathbb{F}_{3^n}$ such that $\mathcal{F}(X) = Y$, and, for each X, we compute $\mathbf{x} = \phi(X) \in \mathbb{F}_3^n$. Finally, we compute $\mathbf{m} = \mathcal{L}_2^{-1}(\mathbf{x})$. If $\mathbf{m} \in \mathcal{M}$; then we output $\mathbf{m}$ as the plaintext. If we fail to derive a vector in $\mathcal{M}$ form all the preimages X, we output the symbol $\perp$ designating an invalid ciphertext.

Why Decryption Works. We just observe that $m_i = 0, 1$, so $m_i^2 = m_i$. Hence, for $k = 0, 1, \ldots, n-1$,

$$\begin{aligned} c_k = q_k(\mathbf{m}) &= \sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} \beta_{ij}^{(k)} m_i m_j + \sum_{i=0}^{n-1} \rho_i^{(k)} m_i + \delta^{(k)} \\ &= \sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} \beta_{ij}^{(k)} m_i m_j + \sum_{i=0}^{n-1} \left(\alpha_i^{(k)} + \gamma_i^{(k)}\right) m_i + \delta^{(k)} \\ &= \sum_{i=0}^{n-1} \alpha_i^{(k)} m_i^2 + \sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} \beta_{ij}^{(k)} m_i m_j + \sum_{i=0}^{n-1} \gamma_i^{(k)} m_i + \delta^{(k)} \\ &= p_k(\mathbf{m}). \end{aligned} \quad (4)$$

So $\mathbf{c} = \mathcal{Q}(\mathbf{m}) = \mathcal{P}(\mathbf{m}) = \mathcal{L}_1 \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ \mathcal{L}_2(\mathbf{m})$. The modified HFE decryption recovers the plaintext $\mathbf{m}$ by peeling off the composition one by one from the leftmost side.

Remarks. The original HFE scheme [5] works on any field $\mathbb{F}_q$ and its extension $\mathbb{F}_{q^n}$. In fact, the quadratic polynomial map $\mathcal{P}$ is exactly the public key of the original HFE scheme, and the secret key of the original scheme also consists of $\mathcal{F}(X)$, $\mathcal{L}_1^{-1}$, and $\mathcal{L}_2^{-1}$. The encryption of the original HFE scheme is just to compute $\mathbf{c} = \mathcal{P}(\mathbf{m})$, where the plaintext $\mathbf{m}$ is in $\mathbb{F}_q^n$ but not necessarily in $\mathcal{M} = \{0, 1\}^n$. The decryption algorithm of the modified HFE scheme is exactly the original HFE decryption.

2.3. Performance and Comparisons. To make a comparison between the proposed HFE modification and the original HFE schemes in a uniform platform, we consider the HFE scheme defined over $\mathbb{F}_3$ and its extension field $\mathbb{F}_{3^n}$. It can be easily seen that both the modified and the original HFE schemes share a common secret key and decryption algorithm. So both schemes have the same secret key sizes and decryption costs. In the modified scheme, the public key is $\mathcal{Q}$, and hence we need not to store the coefficients of the square terms of the public key $\mathcal{P}$. So the proposed scheme reduces the public key size by $\mathcal{O}(n^2)$ bits. During encryption, the proposed modification HFE scheme does not need to do the square computations, so the proposed encryption reduces the computational costs by $\mathcal{O}(n^2)$ bit operations.

3. Security

We analyze the security of the proposed HFE modified encryption scheme. We first review the basic idea of known attacks and then illustrate why the proposal is secure against these attacks.

3.1. Linearization Equations Attack

Basic Idea. Linearization equations attack [18] was found by Patarin on the Matsumoto-Imai scheme [19]. In the Matsumoto-Imai scheme, a permutation $\mathcal{F}(X) = X^{q^\theta+1}$ over $\mathbb{F}_{q^n}$ with characteristic 2 is defined such that $\gcd(q^n - 1, q^\theta + 1) = 1$, then using two invertible affine transformations $\mathcal{L}_1$

and $\mathscr{L}_2$ to disguise the central map $\mathscr{F}$ into a quadratic map $\mathscr{P}$ over $\mathbb{F}_q$, namely,

$$\mathscr{P} = \mathscr{L}_1 \circ \phi \circ \mathscr{F} \circ \phi^{-1} \circ \mathscr{L}_2. \tag{5}$$

The basic idea of the attack is as follows. Note that $Y = \mathscr{F}(X) = X^{q^\theta+1}$ implies $XY^{q^\theta} - X^{q^{2\theta}}Y = 0$. By setting

$$\begin{aligned} \mathbf{x} &= (x_0, \ldots, x_{n-1}) = \phi(X), \\ \mathbf{y} &= (y_0, \ldots, y_{n-1}) = \phi(Y) = \phi(\mathscr{F}(X)) \\ &= \phi\left(\mathscr{F}\left(\phi^{-1}(\mathbf{x})\right)\right), \end{aligned} \tag{6}$$

we can express $XY^{q^\theta} - X^{q^{2\theta}}Y = 0$ as n bilinear equations about input $\mathbf{x}$ and output $\mathbf{y}$ of function $\phi \circ \mathscr{F} \circ \phi^{-1}$:

$$\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_{ij}^{(k)} x_i y_j = 0, \tag{7}$$

where $i, j, k = 0, \ldots, n-1$ and $a_{ij}^{(k)} \in \mathbb{F}_q$. Given a ciphertext $\mathbf{c} = (c_0, \ldots, c_{n-1}) = \mathscr{P}(\mathbf{m})$, we want to recover the corresponding plaintext $\mathbf{m} = (m_0, \ldots, m_{n-1})$. Note that $\mathbf{m}$ ($\mathbf{c}$, resp.) is an affine transformation $\mathscr{L}_2$ ($\mathscr{L}_1$, resp.) on the input (output, resp.) of the function $\phi \circ \mathscr{F} \circ \phi^{-1}$. So $\mathbf{m}$ and $\mathbf{c}$ satisfy the following n equations derived from the n bilinear equations, namely,

$$\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \alpha_{ij}^{(k)} m_i c_j + \sum_{i=0}^{n-1} \beta_i^{(k)} m_i + \sum_{i=0}^{n-1} \gamma_i^{(k)} c_i + \delta^{(k)} = 0, \tag{8}$$

where $i, j, k = 0, \ldots, n-1$ and all the coefficients in $\mathbb{F}_q$. These n equations are called linearization equations and can be efficiently computed from the public polynomials $\mathscr{P}$. It was shown that the linearization equations have a rank of at least $n - \gcd(n, \theta)$ [20]. So given a ciphertext $\mathbf{c} = (c_0, \ldots, c_{n-1}) = \mathscr{P}(\mathbf{m})$, we only need to solve the n linearization equations to obtain the corresponding plaintext $\mathbf{m} = (m_0, \ldots, m_{n-1})$.

Why the Proposal Is Secure against the Linearization Equations Attack. We first note that the HFE scheme [5] was proposed by Patarin to thwart the linearization equations attack and no known evidence was reported on the existence of linearization equations in the HFE scheme. So the HFE scheme is secure against linearization equations attack. As far as the proposed HFE modification scheme is concerned, we just note that, for any plaintext $\mathbf{m} \in \mathscr{M} = \{0, 1\}^n$, $\mathbf{c} = \mathscr{Q}(\mathbf{m}) = \mathscr{P}(\mathbf{m})$ is a valid ciphertext for both the original FHE scheme and the proposed modification HFE scheme. Therefore, we cannot hope to derive linearization equations from the modified HFE scheme.

3.2. MinRank Attacks

Basic Idea. Without loss of generality, we assume that the two invertible affine transformations $\mathscr{L}_1$ and $\mathscr{L}_2$ are linear [21] and define the terms of

$$\mathscr{F}^*(X) = \sum_{0 \le i \le j < n, q^i + q^j \le D} a_{ij} X^{q^i + q^j} \tag{9}$$

in $\mathscr{F}(X)$ in (1). We then can look at $\mathscr{F}^*$ as a quadratic form about

$$\mathbf{X} = \left(X, X^q, \ldots, X^{q^{n-1}}\right); \tag{10}$$

then we associate with $\mathscr{F}^*$ a symmetric n-dimensional square matrix $\mathbf{F}$ such that

$$\mathscr{F}^*(X) = \mathbf{X}\mathbf{F}\mathbf{X}^T. \tag{11}$$

The symmetric matrix $\mathbf{F}$ is of low rank, and it is the special structure of the symmetric matrix $\mathbf{F}$ that makes the original HFE scheme insecure. We recall $0 \le i \le j < n$, $q^i + q^j \le D$ and denote the smallest integer smaller than or equal to $\log_q(D-1) + 1$ as r, and we will find that all the elements of the last $n-r$ columns (rows, resp.) of $\mathbf{F}$ are zero. So the rank of the symmetric matrix $\mathbf{F}$ is at most r. Loosely speaking, when we apply two linear transformations on the input and output of the map $\mathscr{F}^*$, the rank of the corresponding matrix remains at most r. We define the quadratic part of $\mathscr{P} = \mathscr{L}_1 \circ \phi \circ \mathscr{F} \circ \phi^{-1} \circ \mathscr{L}_2$ as $\mathscr{P}^* = (p_0^*, \ldots, p_{n-1}^*)$, namely, for $k = 0, \ldots, n-1$,

$$p_k^*(\mathbf{x}) = \sum_{i=0}^{n-1} \alpha_i^{(k)} x_i^2 + \sum_{i=0}^{n-2}\sum_{j=i+1}^{n-1} \beta_{ij}^{(k)} x_i x_j. \tag{12}$$

Note that $\mathscr{F}^*(X)$ can be expressed as n homogeneous quadratic polynomials over the base field $\mathbb{F}_q$; then the application of two linear transformations on the input and output of $\mathscr{F}^*(X)$ will also give n homogeneous quadratic polynomials over the base field $\mathbb{F}_q$. That is to say

$$\mathscr{P}^* = \mathscr{L}_1 \circ \phi \circ \mathscr{F}^* \circ \phi^{-1} \circ \mathscr{L}_2. \tag{13}$$

Or equivalently,

$$\mathscr{F}^* = \phi^{-1} \circ \mathscr{L}_1^{-1} \circ \mathscr{P}^* \circ \mathscr{L}_2^{-1} \circ \phi. \tag{14}$$

The above equation says that we can lift the quadratic part $\mathscr{P}^*$ of the public key $\mathscr{P}$ to the extension field $\mathbb{F}_{q^n}$ under some unknown linear transformations to derive $\mathscr{F}^*$ and hence $\mathscr{F}$. Kipnis and Shamir noted [7] that, by lifting the quadratic part $\mathscr{P}^*$ of the public key $\mathscr{P}$ of the HFE scheme to the extension field $\mathbb{F}_{q^n}$, they can find a collection of matrices. The matrix $\mathbf{F}$ is then determined by finding a linear combination of these matrices such that $\mathbf{F}$ has a minimum rank (at most r). Thus by solving the MinRank problem we can determine the matrix $\mathbf{F}$ and the coefficients of the linear transformation $\mathscr{L}_1$. Though the MinRank problem is proven to be NP-complete [22, 23], the reduction to the MinRank problem does impose a serious security threat on the security of the HFE scheme [7, 8].

Why the Proposal Is Secure against the MinRank Attack. To illustrate why the proposed modification of the HFE scheme is secure against the MinRank attack [7, 8], we just need to show that when lifted to the extension field $\mathbb{F}_{3^n}$, the quadratic part of the public key $\mathscr{Q}$ is not connected with a low-rank matrix. We set the quadratic part of the public key $\mathscr{Q}$ as $\mathscr{Q}^* = (q_0^*, q_1^*, \ldots, q_{n-1}^*)$ with

$$q_k^*(\mathbf{x}) = \sum_{i=0}^{n-2}\sum_{j=i+1}^{n-1} \beta_{ij}^{(k)} x_i x_j \tag{15}$$

for $k = 0, \ldots, n-1$. If we lift $\mathcal{Q}^*$ to the extension field and find that the corresponding matrix is not of low rank, we can claim our proposal is secure against the MinRank attack [7, 8]. So we define

$$\mathcal{F}_1(X) = \phi^{-1} \circ \mathcal{L}_1^{-1} \circ \mathcal{Q}^* \circ \mathcal{L}_2^{-1} \circ \phi(X) = \mathbf{X}\mathbf{F}_1\mathbf{X}^T. \quad (16)$$

Now we show that the corresponding matrix $\mathbf{F}_1$ is of not necessarily low rank. We define $\mathcal{S} = (s_0, s_1, \ldots, s_{n-1})$ with

$$s_k(\mathbf{x}) = \sum_{i=0}^{n-1} \alpha_i^{(k)} x_i^2 \quad (17)$$

for $k = 0, \ldots, n-1$, and

$$\mathcal{F}_2(X) = \phi^{-1} \circ \mathcal{L}_1^{-1} \circ \mathcal{S} \circ \mathcal{L}_2^{-1} \circ \phi(X) = \mathbf{X}\mathbf{F}_2\mathbf{X}^T. \quad (18)$$

It is obvious that $\mathcal{P}^*(\mathbf{x}) = \mathcal{Q}^*(\mathbf{x}) + \mathcal{S}(\mathbf{x})$. Thus we can easily verify that

$$\begin{aligned} \mathbf{X}\mathbf{F}\mathbf{X}^T &= \mathcal{F}^*(X) = \phi^{-1} \circ \mathcal{L}_1^{-1} \circ \mathcal{P}^* \circ \mathcal{L}_2^{-1} \circ \phi(X) \\ &= \phi^{-1} \circ \mathcal{L}_1^{-1} \circ \left(\mathcal{Q}^* + \mathcal{S}\right) \circ \mathcal{L}_2^{-1} \circ \phi(X) \\ &= \phi^{-1} \circ \mathcal{L}_1^{-1} \circ \mathcal{Q}^* \circ \mathcal{L}_2^{-1} \circ \phi(X) + \phi^{-1} \circ \mathcal{L}_1^{-1} \\ &\quad \circ \mathcal{S} \circ \mathcal{L}_2^{-1} \circ \phi(X) = \mathcal{F}_1(X) + \mathcal{F}_2(X) \\ &= \mathbf{X}\mathbf{F}_1\mathbf{X}^T + \mathbf{X}\mathbf{F}_2\mathbf{X}^T = \mathbf{X}\left(\mathbf{F}_1 + \mathbf{F}_2\right)\mathbf{X}^T. \end{aligned} \quad (19)$$

So we get $\mathbf{F}_1 = \mathbf{F} - \mathbf{F}_2$. In this matrix equation, we only know that $\mathbf{F}$ is of low rank (at most r). However, the rank of the matrix $\mathbf{F}_2$ is unknown, and hence the rank of the matrix $\mathbf{F}_1$ is not necessarily low. So the adversary cannot derive from the publicly known map $\mathcal{Q}^*$ a low-rank matrix. So the MinRank attack does not apply to cryptanalyzing the proposed HFE modification scheme.

3.3. Algebraic Attacks

Basic Idea. One straightforward way to attack multivariate public key cryptosystems is to directly solve the multivariate quadratic equations by utilizing some algorithms to compute the Gröbner basis of some ideals. Given the ciphertext $\mathbf{c} = \mathcal{Q}(\mathbf{m})$, we want to solve the plaintext $\mathbf{m}$ from the quadratic equations:

$$\begin{aligned} q_0(m_0, m_1, \ldots, m_{n-1}) &= c_0, \\ q_1(m_0, m_1, \ldots, m_{n-1}) &= c_1, \\ &\vdots \\ q_{n-1}(m_0, m_1, \ldots, m_{n-1}) &= c_{n-1}. \end{aligned} \quad (20)$$

The algebraic or the direct attacks can use some Gröbner basis algorithms such as **F**5 [24] and the XL [25] algorithms to solve the generators for the ideal $\mathcal{I} = \langle q_0 - c_0, q_1 - c_1, \ldots, q_{n-1} - c_{n-1} \rangle$ generated by $q_0 - c_0, q_1 - c_1, \ldots, q_{n-1} - c_{n-1}$. It is observed [26] that the field equations $m_i^q - m_i = 0$ for $i = 0, 1, \ldots, n-1$ will be useful to simplify the computations, so we also can add the n field equations to the generators; namely, we solve the Gröbner basis of the ideal

$$\begin{aligned} \mathcal{I}^* = \langle & q_0 - c_0, \ldots, q_{n-1} - c_{n-1}, m_0^q - m_0, \ldots, m_{n-1}^q \\ & - m_{n-1} \rangle. \end{aligned} \quad (21)$$

Why the Proposal Is Secure against the Algebraic Attack. In the proposed modification HFE encryption scheme, we impose some restrictions on the plaintext space. The plaintext space is $\mathcal{M} = \{0, 1\}^n$ but not $\mathbb{F}_3^n$. Thus we have some additional equations that associate with the plaintext $\mathbf{m} = (m_0, m_1, \ldots, m_{n-1})$; namely, for $i = 0, q, \ldots, n-1$, we have $m_i^2 - m_i = 0$. The plaintext block m_i also satisfies the field equation $m_i^3 - m_i = 0$. However, we can derive the field equations $m_i^3 - m_i = 0$ from the equations $m_i^2 - m_i = 0$. So in the proposed modification encryption scheme, we need to find the Gröbner basis for the ideal

$$\begin{aligned} \mathcal{I}' = \langle & q_0 - c_0, \ldots, q_{n-1} - c_{n-1}, m_0^2 - m_0, \ldots, m_{n-1}^2 \\ & - m_{n-1} \rangle. \end{aligned} \quad (22)$$

To evaluate the difficulty of the Gröbner basis algorithms to recover the plaintext, we can use the degree of regularity D_{reg} of the quadratic equations [27] to estimate the computational costs. The computational costs are at least $\mathcal{O}(n^{2D_{\text{reg}}})$ bit operations, according to the results given on page 219 in [2]. Under the suggested parameters $n = 256$ and $D = 144$, the degree of regularity of the quadratic equations is $D_{\text{reg}} = 5$. So the computational overhead is about $256^{10} = 2^{80}$ bit operations. So under the algebraic attacks, the proposed modification HFE encryption scheme can obtain a security level of 80 bits under the suggested parameters.

3.4. Suggested Parameters.

Considering the aforementioned discussions, we suggest choosing $n = 256$ and $D = 144$. We can see from the security analysis that the proposed HFE modification encryption scheme can obtain a security level of 80 bits under the suggested parameters.

4. Conclusions

In this paper, we proposed a novel modified HFE encryption scheme. The proposed HFE modification has the following features:

(i) *Universal padding scheme for multivariate public key encryptions*: the proposed HFE variant can merge the square and linear terms by imposing some restrictions on the plaintext space. The proposed method is a universal padding scheme and hence can be used to other multivariate cryptographic constructions.

(ii) *Fully nonlinear transformation on the central map*: the proposed method can remove all the square terms in the public multivariate quadratic polynomials and thus impose a nonlinear transformation on all the polynomials.

(iii) *Security against known attacks*: we illustrated that the proposed HFE modification encryption scheme is secure against known attacks including the linearization equation attack, the MinRank attack, and the algebraic attacks.

(iv) *More efficient encryption and smaller public key size*: the proposed modification encryption scheme does not store the square terms in the public key and hence can reduce the encryption costs by $\mathcal{O}(n^2)$ bit operations and saves the public key storage by $\mathcal{O}(n^2)$ bits.

As a new multivariate public key encryption, the security of the proposal needs to be furthered. So we encourage the readers to examine the security of the proposal.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by National Natural Science Foundation of China (Grants nos. 61572390, 61303232, and 61540049), National Key Research and Development Program of China (no. 2017YFB0802002), Natural Science Foundation in Ningbo of China (no. 201601HJ-B01382), Program for Science & Technology Innovation Talents in Universities of Henan Province (no. 18HASTIT022), Foundation of Henan Educational Committee (Grants nos. 16A520025 and 18A520047), Foundation for University Key Teacher of Henan Province (no. 2016GGJS-141), Open Foundation of Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education (Guilin University of Electronic Technology) (no. CRKL160202), and Outstanding Young Teacher Project of Xuchang University.

References

[1] N. Koblitz and A. J. Menezes, "A survey of public-key cryptosystems," *SIAM Review*, vol. 46, no. 4, pp. 599–634, 2004.

[2] J. Ding, J. E. Gower, and D. S. Schmidt, *Multivariate Public Key Cryptosystems*, vol. 25 of *Advances in Information Security*, Springer, New York, Berlin, Germany, 2006.

[3] Y. Zou, W. Ma, Z. Ran, and S. Wang, "New multivariate hash function quadratic polynomials multiplying linear polynomials," *IET Information Security*, vol. 7, no. 3, pp. 181–188, 2013.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[5] J. Patarin, "Hidden fields equations (HFE) and isomorphism of polynomials (IP): two new families of asymmetric algorithms," in *Proceedings of Advances in Cryptology-Eurocrypt 1996*, vol. 1070, pp. 33–48, Springer-Verlag, Saragossa, Spain, 1996.

[6] E. R. Berlekamp, "Factoring polynomials over finite fields," *The Bell System Technical Journal*, vol. 46, pp. 1853–1859, 1967.

[7] A. Kipnis and A. Shamir, "Cryptanalysis of the HFE public key cryptosystem by relinearization," in *Proceedings of the Advances in Cryptology-Crypto 1999*, vol. 1666, pp. 19–30, Springer, Berlin, Santa Barbara, CA, USA, 1999.

[8] J. C. Faugère and A. Joux, "Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases," in *Proceedings of the Advances in Cryptology-Crypto 2003*, vol. 2729, pp. 44–60, Springer-Verlag, Santa Barbara, USA, 2003.

[9] N. Courtois, "The security of Hidden Field Equations (HFE)," in *Proceedings of the Topics in Cryptology-CT-RSA 2001*, vol. 2020, pp. 266–281, Springer-Verlag, San Francisco, CA, USA.

[10] J. Patarin, N. Courtois, and L. Goubin, "QUARTZ, 128-bit long digital signatures," in *Proceedings of the Topics in Cryptology-CT-RSA 2001*, vol. 2020, pp. 282–297, Springer-Verlag, San Francisco, CA, USA.

[11] O. Billet, J. Patarin, and Y. Seurin, "Analysis of intermediate field systems," 2013, http://eprint.iacr.org/2009/542.

[12] C. Chen, M. S. Chen, and J. Ding, "Odd-char multivariate hidden field equations," 2013, http://eprint.iacr.org/2008/543.

[13] J. Ding, D. Schmidt, and F. Werner, "Algebraic attack on HFE revisited," in *Proceedings of the International Conference on Information Security-ISC 2008*, vol. 5222, pp. 215–227, Springer-Verlag, Taipei, China, 2008.

[14] C. Wolf and B. Preneel, "Taxonomy of public key schemes based on the problem of multivariate quadratic equations," 2013, https://eprint.iacr.org/2005/077.

[15] N. T. Courtois, M. Daum, and P. Felke, "On the security of HFE, HFEv- and Quartz," in *Proceedings of the International Conference on Practice and Theory in Public Key Cryptography-PKC 2003*, vol. 2567, pp. 337–350, Springer-Verlag, Miami, Fl, USA, 2003.

[16] L. Bettale, J. C. Faugère, and L. Perret, "Cryptanalysis of HFE, Multi-HFE and variants for odd and even characteristic," *Designs, Codes and Cryptography*, vol. 69, no. 1, pp. 1–52, 2013.

[17] L. Bettale, J.-C. Faugère, and L. Perret, "Cryptanalysis of multivariate and odd-characteristic hfe variants," in *Proceedings of the International Conference on Practice and Theory in Public Key Cryptography-PKC 2011*, vol. 6571, pp. 441–458, Springer, Heidelberg.

[18] J. Patarin, "Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88," in *Advances in cryptology-CRYPTO '95*, vol. 963, pp. 248–261, Springer, Berlin, Santa Barbara, CA, USA, 1995.

[19] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," in *Advances in cryptology-EUROCRYPT '88*, vol. 330, pp. 419–453, Springer, Berlin, Davos, Switzerland, 1988.

[20] A. Diene, J. Ding, J. E. Gower, T. J. Hodges, and Z. Yin, "Dimension of the linearization equations of the Matsumoto-Imai cryptosystems," in *Proceedings of the International Workshop on Coding and Cryptography-WCC 2005*, vol. 3969, pp. 242–251, Springer-Verlag, Bergen, Norway, 2005.

[21] L. Perret, "A fast cryptanalysis of the isomorphism of polynomials with one secret problem," in *Proceedings of the Advances in Cryptology-Eurocrypt 2005*, vol. 3494, pp. 354–370, Springer-Verlag, Aarhus, Denmark, 2005.

[22] J. F. Buss, G. S. Frandsen, and J. O. Shallit, "The computational complexity of some problems of linear algebra (extended abstract)," in *Proceedings of the Symposium on Theoretical Aspects of Computer Science-STACS 1997*, vol. 1200, pp. 451–462, Springer-Verlag, Lübeck, Germany, 1997.

[23] J.-C. Faugère, M. S. El Din, and P.-J. Spaenlehauer, "On the complexity of the generalized MinRank problem," *Journal of Symbolic Computation*, vol. 55, no. 1, pp. 30–58, 2013.

[24] J.-C. Faugère, "A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)," in *Proceedings of the 2002 International Symposium on Symbolic And Algebraic Computation-ISSAC 2002*, pp. 75–83, ACM Press, New York, NY, USA, 2002.

[25] N. Courtois, A. Klimov, J. Patarin et al., "Efficient algorithms for solving overdefined systems of multivariate polynomial equations," in *Proceedings of the Advances in Cryptology-Eurocrypt 2000*, vol. 1807, pp. 392–407, Springer-Verlag, Bruges, Belgium, 2000.

[26] N. T. Courtois and J. Patarin, "About the XL algorithm over GF(2)," in *Proceedings of the Topics in Cryptology-CT-RSA 2003*, vol. 2612, pp. 141–157, Springer-Verlag, San Francisco, CA, USA, 2003.

[27] V. Dubois and N. Gama, "The degree of regularity of HFE systems," in *Proceedings of the Advances in Cryptology-Asiacrypt 2010*, vol. 6477, pp. 557–576, Springer-Verlag, Singapore, 2010.